The Commonwealth of Massachusetts
AUDITOR OF THE COMMONWEALTH
ONE ASHBURTON PLACE, ROOM 1819
BOSTON, MASSACHUSETTS 02108
TEL. (617) 727-6200

A. JOSEPH DeNUCCI
AUDITOR

No. 2002-0247-4T

OFFICE OF THE STATE AUDITOR'S REPORT ON INFORMATION TECHNOLOGY-RELATED CONTROLS AT THE DEPARTMENT OF MENTAL RETARDATION REGION III

July 1, 2001 through November 30, 2001

OFFICIAL AUDIT REPORT

MAY 13, 2002

2002-0247-4T

TABLE OF CONTENTS

INTRODUCTION

The Department of Mental Retardation (DMR) is organized under Chapter 19B, Sections 1 to 18, of the Massachusetts General Laws and is placed within the purview of the Executive Office of Health and Human Services. The DMR is comprised of twenty-six area offices that operate within five regions located throughout the Commonwealth.

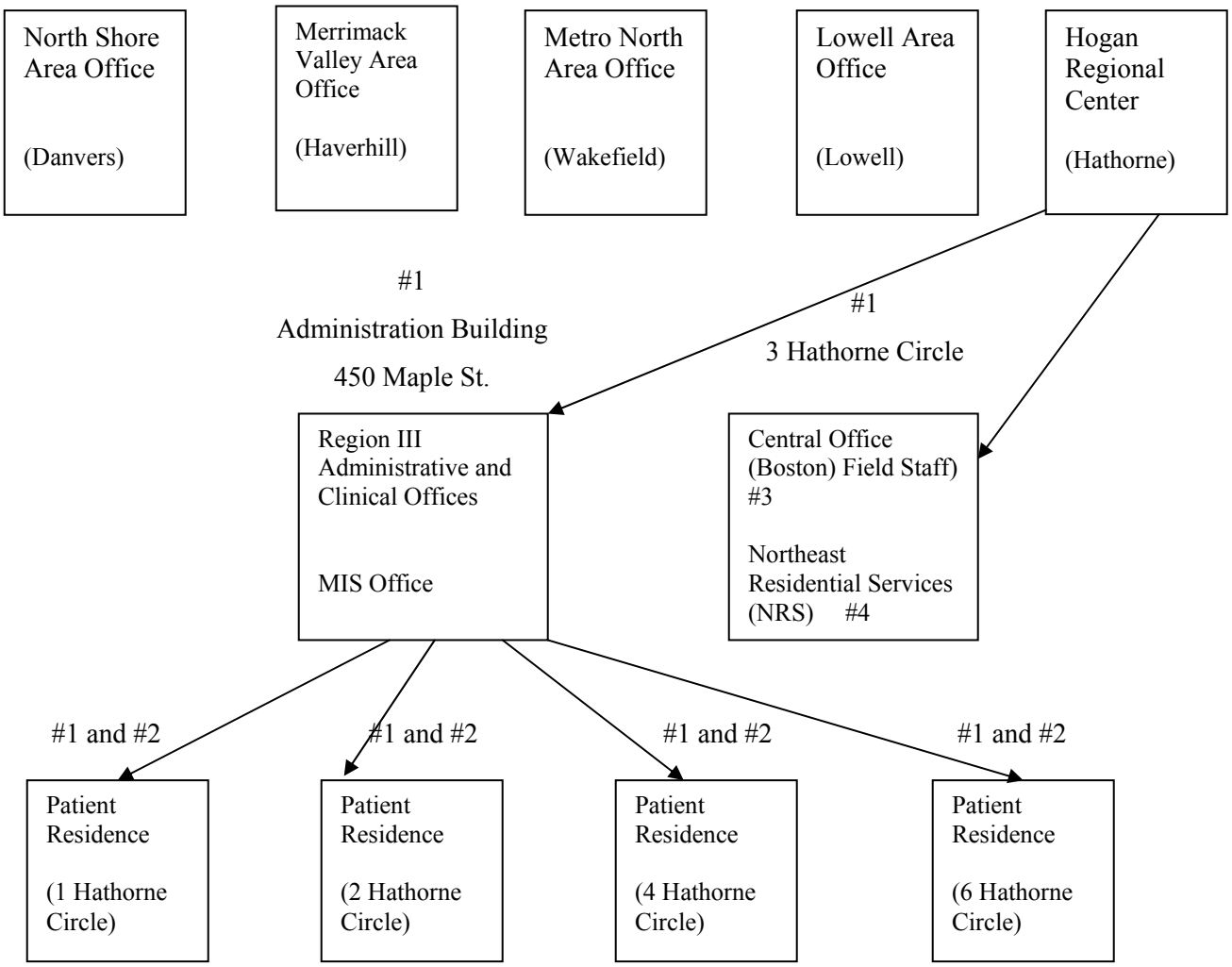
DMR's primary mission is to provide a variety of support services, such as residential services, employment assistance, help for families to care for family members at home, transportation, treatment, monitoring, and care to the Commonwealth's mentally retarded citizens. Through various state-operated programs and contracts with 265 private providers, DMR assists approximately 30,000 clients each year. In conjunction with community-based programs, DMR serves approximately 1,199 clients in seven developmental centers, such as Monson Developmental Center, Glavin Regional Center, and the Hogan Regional Center.

DMR's Region III, also known as the Northeast Region, includes 50 cities and towns in Essex County and certain areas of Middlesex County. Region III is comprised of four area offices located in Danvers, Haverhill, Lowell, and Wakefield and the Hogan Regional Center facility in Hathorne and provides services to 6,579 clients. The Northeast Regional Office is located on the grounds of the Hogan Regional Center. The regional office is responsible for the management of the Hogan Regional Center facility and community-based programs in the cities and towns located within Region III. Regarding housing options, Region III manages 42 state-operated community homes that provide services to 199 clients and contracts with 43 vendors who provide services in over 582 residential locations to 1,170 clients. In addition, the Hogan Regional Center provides residential services to 152 clients, various day services to live-in clients and community residents, and short-term evaluation and treatment. (See Figure 1, page 2 for a graphical representation of the physical organization of Region III.)

At the time of our audit, 1,249 Department staff were employed in Region III. The staff included 489 staff who work at the Hogan facility, 188 who work for the regional area offices, and 572 who work for the Northeast Regional Services (NRS) that operate state-sponsored community homes. In addition, 21 staff from central office departments in Boston, such as investigations, legal, and human rights were located at the regional office.

Figure 1

Department of Mental Health
Physical Organization of Region III Area Offices and Facilities
Northeast Region



Notes

#1: Administration building, 3 Hathorne Circle, and the patient residences are located on the grounds of the Hogan Regional Center

#2: The patient residences are physically connected to the Administration building

#3: Central Office field staff assigned to Region III: (a). Investigations, (b). Legal, (c). Quality Enhancements, and (d). Human Rights

#4: NRS staff manage state-operated community homes throughout Region III

DMR's computer operations are supported by file servers and microcomputer systems configured in local area networks (LAN) that are located at the regional and area offices. These file servers are connected through telecommunication lines to two file servers at the DMR central office in Boston through which Internet access is provided. The central office's SQL server processes applications such as Impact, which is an accounting application used in conjunction with the Massachusetts Management and Accounting Reporting System (MMARS) to account for managers' expenditures, investigations of abuse, and various billing systems. The Notes server processes applications such as critical incident reports, individual service plans, and risk management. The file servers are connected through a wide area network (WAN) to the Information Technology Division's (ITD) mainframe, which provides connectivity for access to the Human Resource Compensation Management System (HR/CMS). Critical applications such as MMARS and DMR's client registry system operate on ITD's mainframe.

Our Office's examination focused on selected general controls such as physical security and environmental protection, system access security, inventory control over IT-related resources, and business continuity planning, including on-site and off-site storage.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

From October 22, 2001 through November 30, 2001, we performed an audit of selected information technology (IT)-related controls at the Department of Mental Retardation's (DMR) Region III (Northeast Region) for the period covering July 1, 2001 through November 30, 2001. The scope of our audit included an examination of control practices, procedures, and devices regarding physical security and environmental protection over and within the administration building at the Hogan Regional Center facility that houses certain administrative offices and the Management Information Systems (MIS) office for the Northeast Region. Further, we reviewed physical security and environmental protection over the automated systems installed at the North Shore and Merrimack Valley area offices located in Danvers and Haverhill, respectively. We reviewed physical security and environmental protection over restricted areas housing confidential client records at the two area offices.

Our audit included a review and evaluation of system access security to the DMR's application systems and a review of access controls over the network on which the applications reside. We reviewed control practices regarding the accounting for IT-related resources, including computer equipment located in the administration building at the Hogan facility and the two area offices. In conjunction with our audit, we reviewed formal policies and procedures promulgated by DMR regarding controls and operations for the areas under our review.

Regarding system availability, we reviewed business continuity planning for the daily casework and administrative and financial operations processed through the automated systems. With respect to the restoration of normal business functions, we reviewed the adequacy of formal policies and procedures regarding business continuity planning and the physical security and environmental protection of backup media stored on-site at Hogan Regional Center and North Shore and Merrimack Valley area offices we visited.

Audit Objectives

Our primary audit objective was to determine whether adequate security controls were in place and in effect to provide reasonable assurance that only authorized parties could access the application systems and IT resources and that system information was sufficiently protected against unauthorized disclosure, change, or deletion. In addition, we determined whether adequate controls had been implemented to provide reasonable assurance that only authorized

users were granted access to the DMR's applications and that unauthorized access was prevented or detected. We sought to determine whether adequate physical security and environmental protection were in place to restrict access to IT resources, including confidential client records in hardcopy form, to only authorized users in order to prevent unauthorized use, damage, or loss of IT resources. A further objective was to determine whether adequate control practices were in place and in effect regarding the proper accounting for IT-related resources in Hogan's administration building and the North Shore and Merrimack Valley area offices. We sought to determine whether adequate business continuity planning had been performed and whether plans were in place to restore mission-critical and essential business operations in a timely manner should the application systems processed on the file servers at DMR's central office or file servers and associated microcomputer systems at the Hogan facility and/or area offices be inoperable or unavailable for an extended period. We reviewed the impact of loss of applications such as the client registry system and MMARS-related accounting applications operating on ITD's mainframe. Further, we determined whether physical security and environmental protection regarding on-site storage areas for computer-related media were adequate. We did not review the off-site storage location for DMR's data and applications processed at the Hogan facility and the central office or through the ITD mainframe.

Audit Methodology

To determine the areas to be examined during our IT audit, we performed a preliminary review of internal controls related to physical security and environmental protection over and within the administration building at the Hogan Regional Center. We conducted additional pre-audit work, which included reviewing the role of the regional office regarding physical security and environmental protection over automated systems installed at business offices and the MIS office at the Hogan facility and North Shore and Merrimack Valley area offices. In addition, we interviewed DMR management to discuss internal controls regarding physical security and environmental protection over hardcopy client records located at Hogan and area offices and over on-site and off-site storage of critical computer-related backup media at Hogan and the area offices. Further, we inspected the administrative offices and the MIS office located in the administration building, interviewed DMR management and staff, observed selected operations, reviewed relevant documents such as DMR's internal control plan and the Department's network configuration, and performed selected audit tests. Prior to the inception of our substantive audit work, we discussed the scope and objectives of our audit with senior management at the Region III.

We determined whether DMR's central office in Boston had developed and implemented written, authorized, and approved policies and procedures regarding physical security, environmental protection, system access security and security over client records in accordance with regulatory requirements. In addition, we determined whether Region III had developed written internal control documentation. We determined whether the internal control documentation for the areas under review provided management and users sufficient standards and guidelines to describe, review, and comply with statutes, regulations and generally accepted control objectives for IT operations and security.

To determine whether physical access over IT-related resources, including computer equipment, was restricted to only authorized users and that these IT resources were adequately safeguarded from loss, theft, or damage, we performed audit tests at the Hogan administration building and the North Shore and Merrimack Valley area offices. We reviewed physical security and environmental protection controls over IT-related equipment through inspection and interviews with DMR management and staff. We interviewed the operations manager responsible for physical security and the engineer and electrician responsible for environmental protection at the Hogan Regional Center. Further, we interviewed the area office director at the Merrimack Valley area office and the administrative assistant at the North Shore area office responsible for physical security. We reviewed and evaluated physical security over the MIS office at the Hogan facility, including the room housing the file server. To determine whether adequate controls were in effect to prevent and detect unauthorized access to business offices at the Hogan administration building and area offices housing automated systems, we inspected physical access controls, such as appropriately-locked entrance and exit doors, the presence of a receptionist, burglar alarms, and whether visitor badges were being issued.

Regarding key management at the Hogan Regional Center, we interviewed the locksmith responsible for maintaining records of staff issued keys for the administration building's outside doors and to business offices within the buildings. Further, we interviewed the operations manager regarding controls over key distribution and return. We reviewed written procedures regarding the issuance of keys to DMR and outsourced staff. We also reviewed procedures followed to distribute keys to authorized staff.

To determine whether adequate controls were in effect to physically secure confidential client records, we inspected restricted areas within the business offices where confidential client records were stored. We reviewed sign-out/sign-in procedures for client records at the two area offices.

To determine whether adequate environmental protection controls were in place to properly safeguard automated systems from loss or damage, we checked for the presence of fire detectors

and alarms, fire control methods such as sprinklers and inert-gas fire suppression systems, power surge protection, and emergency power generators and lighting at the administration building and the two area offices we visited. We reviewed general housekeeping procedures to determine whether only appropriate office supplies and equipment were placed in computer rooms or in the vicinity of IT-related equipment. To determine whether proper temperature and humidity controls were in place, we reviewed for the presence of appropriate dedicated air-conditioning units in business offices, computer rooms, and on-site storage areas. Further, we reviewed control procedures to prevent water damage to automated systems, client records, and IT-related backup media for on-site storage.

Our tests of system access security included a review of access privileges of those employees authorized to access the network and associated microcomputer systems. To determine whether DMR control practices regarding system access security adequately prevents unauthorized access to automated systems, we reviewed policies and procedures regarding system access and data security, interviewed the DMR's Chief Information Officer (CIO) at the central office and the Director of MIS responsible for system access security at the Hogan facility and area offices within Region III.

To determine whether the administration of logon ID and passwords was being properly carried out, we initially reviewed internal control documentation regarding system access security. We then reviewed the security procedures with the Region III's Director of MIS responsible for access to the automated systems on which the DMR's application systems operate. In addition, we reviewed control practices used to assign DMR staff access to the application programs and data files. To determine whether controls in place were adequate to ensure that access privileges to the automated systems were granted only to authorized users, we reviewed and evaluated procedures for authorizing, activating, and deactivating access to DMR's application software and related data files. We then confirmed a judgmental sample of active user accounts to documentation authorizing the users to access DMR's automated systems. Because DMR was upgrading its network software, the Department was unable to provide an automated record of individuals with active access privileges in a timely manner. As a result, we could not compare users with active access privileges to DMR's personnel roster of current employees to determine whether all users with active privileges were current employees. However, we determined whether all employees authorized to access the automated systems were required to change their passwords periodically and, if so, the frequency of the changes. We reviewed control practices regarding the detection of unauthorized attempts to access the DMR's network and applications.

To assess the adequacy of business continuity planning, we determined whether any formal planning had been performed to resume computer operations should automated systems be rendered inoperable or inaccessible. In addition, we interviewed the CIO at DMR's central office and the Director of MIS at the Hogan facility to determine whether a written, tested business continuity plan was in place, whether the criticality of application systems had been assessed, and whether risks and exposures to computer operations had been evaluated. Moreover, to evaluate the adequacy of controls to protect LAN- and microcomputer-based data files and software, we interviewed DMR staff responsible for creating backup copies of IT-related media at the Hogan facility and two area offices we visited. We inspected the storage locations for the on-site backup media at the Hogan facility and the two area offices. We did not inspect the off-site storage of backup media for the regional offices.

To determine whether adequate controls were in place and in effect to properly account for IT-related resources at Region III, we reviewed and evaluated the appropriateness of the inventory control practices and procedures. We determined whether computer equipment was properly tagged with state identification numbers and that the tag numbers were accurately recorded on the inventory record. In addition, we determined whether the serial numbers attached to the computer equipment were accurately recorded on the hardware inventory record. We reviewed the inventory record's data fields for item description, serial number, cost, and location.

To determine whether the IT-related inventory record, dated October 30, 2001 and valued at $468,742, were current, accurate, and complete, we confirmed the inventory list provided by the auditee to the actual computer equipment on hand. Region III maintains an inventory record for the Northeast Region, including the Hogan Regional Center and the four area offices. We chose a judgmental sample of 30 (14.5%) of 207 pieces of computer equipment located in the administration building and the MIS office at the Hogan Regional Center. We compared the tag numbers attached to the computer equipment to the corresponding numbers listed on the hardware inventory record. In addition, we selected 18 pieces of computer equipment purchased during the 1998 through 2001 fiscal years and compared purchase documentation to the inventory record and then to the actual equipment on hand. Further, we traced an additional judgmental sample of hardware items to the inventory record. To perform an additional compliance test, we traced 106 (65%) of 162 central processing units, valued at $137,856 listed on surplus property records to the inventory record and to the actual equipment on hand. To determine whether adequate controls had been implemented to provide reasonable assurance that LAN- and microcomputer-based software would be properly accounted for, we reviewed software inventory control practices and procedures.

To determine whether IT-related resources were properly accounted for at the North Shore area office we confirmed 34 (37%) of 91 pieces of equipment valued at $43,770 to the inventory record. Because the inventory record maintained at the Merrimack Valley area office did not identify the actual location of the IT equipment in the "location" data field, our test of inventory was limited to comparing information on a judgmental sample of 34 (41%) of 83 pieces of equipment valued at $33,265 to the inventory record.

To assess business continuity efforts, we reviewed the adequacy of formal planning to resume mission-critical and essential operations should the file server and the microcomputer systems installed at the Hogan Regional Center be damaged or destroyed. We interviewed the Director of MIS at Region III and the DMR's CIO to determine whether the criticality of application systems had been assessed, whether risks and exposures to computer operations had been evaluated, and whether a written business continuity plan was in place. In addition, to determine whether controls were adequate to ensure that data files and software for DMR applications would be available should the automated system be rendered inoperable, we interviewed DMR management responsible for creating backup copies of computer-related media at the Hogan Regional Center and the two area offices reviewed. Further, we reviewed the adequacy of provisions for on-site and off-site storage of critical and important backup tapes at the Hogan Regional Center and two area offices. We reviewed and evaluated the adequacy of physical security and environmental protection controls for the on-site storage locations at Hogan and the two area offices. We did not review the adequacy of on-site or off-site storage for applications processed on the two file servers at DMR's central office or the off-site location for applications processed on the ITD mainframe.

Our audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) of the United States and generally accepted computer industry control practices and auditing standards.

AUDIT SUMMARY

Based on our audit, adequate controls were found to be in place to provide reasonable assurance that IT-related resources at the Department of Mental Retardation's (DMR) Region III, specifically the administration building at the Hogan Regional Center and the North Shore and Merrimack Valley area offices, were properly safeguarded and accounted for. Our audit indicated that appropriate controls were in place regarding logon ID and password administration to provide reasonable assurance that only authorized users were granted access to application systems and the network on which they operated. Further, nothing came to our attention to indicate that system information was not adequately protected against unauthorized disclosure, change, or deletion.

We found that DMR had implemented adequate physical security controls to provide reasonable assurance that only authorized persons could access business offices, computer rooms, and automated systems at the North Shore and Merrimack Valley area offices. We determined that security over hardcopy confidential information at the two area offices we visited was adequate. Although we found that important physical security controls were in place over and within the administration building at the Hogan facility to provide reasonable assurance that only authorized persons could access business offices, computer rooms, and automated systems, we determined that controls regarding key management needed to be strengthened. Our audit indicated that adequate environmental protection was in place over file servers and associated microcomputer systems installed in the administration building at the Hogan Regional Center and the two area offices to provide reasonable assurance that loss or damage to IT-related resources would be prevented.

Regarding business continuity planning, our audit indicated that although Region III had implemented certain informal procedures regarding alternate processing sites and user area plans, a current, tested business continuity plan was not in place. In addition, we determined that on-site storage for important computer-related media at the Hogan facility and the North Shore and Merrimack Valley area offices needed to be improved.

Our review of the DMR's internal control structure indicated that senior management was aware of the need for internal controls and had implemented significant controls to safeguard and account for Region III's IT-related assets. We determined that there was a defined organizational structure, an established chain of command, clear assignment of responsibilities, and documented job descriptions. With respect to appropriate use of information technology, we determined that the Department had promulgated adequate written policies and procedures regarding e-mail and Internet use. However, our audit revealed that although DMR had

promulgated an internal control plan, Region III needed to enhance documented controls by detailing more specific control practices and operating procedures regarding physical security and environmental protection, logon ID and password administration, and business continuity planning.

Our audit disclosed that Region III's inventory control procedures provided reasonable assurance that IT-related resources, including computer equipment installed in the administration building at the Hogan facility and the North Shore and Merrimack Valley area offices, were properly accounted for. We found that Region III had designated a staff person to maintain the inventory record. Significant items of computer equipment were tagged. The inventory record included appropriate data fields such as tag number, serial number, and cost. Based on tests of computer equipment in the administration building and the two area offices, we determined that the inventory record as of October 30, 2001, valued at $468,742, was current, accurate, and complete. Further, we found that surplus property was properly accounted for in Department records.

With respect to system access security, our audit disclosed that the processes for granting and recording authorization, activating, and deactivating users were appropriate. We determined that users with active access privileges were properly authorized, logon IDs and passwords were assigned to users, and access levels to DMR applications were assigned to users based upon "work groups." At the time of our audit, DMR could not provide us with a list of users with access privileges to application systems because of an upgrade to network software. Because the list of active users could not be provided in a timely manner, we could not determine whether all persons with active privileges were current employees. Further, we determined that DMR had not regularly monitored unauthorized attempts to access the network. To improve controls over system access, we recommend that DMR implement procedures to monitor and report on access attempts and resolution of security violations and violation attempts. The control procedures should be documented in the internal control plan. Further, we recommend that DMR ensure that control documentation adequately addresses password formation and use, length of passwords, and frequency of password change. We recommend that DMR determine an appropriate interval regarding password change. Regarding data confidentiality, we determined that DMR was aware of its responsibility for protecting confidentiality of client information.

We determined that important physical security controls were being provided within the area offices we visited to restrict access to authorized users and to prevent loss or disclosure of hardcopy confidential client records. However, we found that physical security over the file server at North Shore area office needed to be improved. To strengthen controls, we recommend

that the file server at the North Shore area office be installed in an office areas not used for other purposes.

Our audit indicated that adequate environmental protection such as fire detectors and alarms, sprinkler systems, and an uninterruptible power supply (UPS) to prevent loss of data should power suddenly fail, were in place at the areas offices to prevent damage to, or loss of, IT-related resources. Further, we found that adequate environmental protection such as fire detectors and alarms, emergency power supply, UPS, and fire extinguishers in the MIS office were in place in the administration building at the Hogan Regional Center. We determined that the file server at the Hogan facility was subject to air quality and temperature monitoring and that an alarm system was in place. According to DMR management, regular inspection and maintenance programs were in place for fire alarms, emergency power supply, UPS, and heat, ventilation, and air-conditioning systems. We recommend that DMR management include control procedures, such as instructions and schedules to perform inspections and maintenance of fire alarms and UPS, and emergency evacuation procedures in the internal control plan.

Our audit revealed that appropriate and important physical security controls were in place over and within the administration building at the Hogan Regional Center. These controls included continuous foot patrols by state police on the grounds of the Hogan Regional Center and within the administration building, telephone operators on duty 24 hours a days, seven days a week in the administration building, business office doors locked after normal business hours, and a sign-in log required for visitors after normal business hours. Further, we found that the file server was located in a room that was difficult to access from outside the building and was kept in a locked cabinet. To further strengthen physical security, we recommend that the sign-in log be used during regular business hours, identification badges for staff and visitors be used, and the door to the MIS office be closed during normal business hours if the staff is not present.

Regarding key management, we determined that although DMR had implemented important controls regarding the distribution of outside keys to the administration building at the Hogan facility, certain controls needed to be improved. In addition to the physical security controls noted above, we found that both the administration building and the connecting facility housing residents were staffed 24 hours a day, seven days a week. It is our understanding that DMR staff, parents, and other individuals issued outside keys have access only to areas within the administration building and residence that are continually staffed. According to DMR management, key distribution procedures were in compliance with Title XIX regulations for a long-term facility serving individuals with extensive disabilities. DMR management was able to account for 650 keys that, according to locksmith records, were currently distributed to staff.

To strengthen control practices regarding key management, we recommend that DMR maintain a master list of all individuals who are issued keys; sequentially number "open request" forms for keys; periodically review records to determine individuals who have not returned keys; and, notify on-site personnel, including the operations manager and state police regarding individuals who have not returned keys. Further, we recommend that keys be stamped "do not duplicate." We determined that control practices regarding the distribution of keys to the business offices and the MIS office in the administration building were adequate.

With respect to business continuity planning, we determined that DMR's Region III had performed certain preliminary steps regarding the development of a business continuity plan. However, Region III management, in conjunction with DMR's central office, needed to document procedures to restore normal business functions in a timely manner, should automated systems be unavailable for an extended period. For instance, we determined that Region III management had informally designated certain applications, such as critical incident reports, individual service plans for DMR clients, and the client-related data warehouse processed on the DMR central office's file servers and the consumer registry system operating on the ITD mainframe as critical systems related to client services. Further, Region III had developed informal procedures to process various transactions at alternate sites should automated systems at the Hogan facility or area offices or telecommunication links to the central office be unavailable for an extended period. According to DMR management, the alternate processing sites had been successfully used.

We acknowledge that DMR's central office has implemented control procedures such as redundant file servers, daily electronic backup of regional and area office file servers, and weekly off-site storage for central office and regional office backup that would help to restore normal business functions should file servers or telecommunication links to the central office be unavailable. We believe that Region III and the central office have developed significant elements of a business continuity plan. However, to achieve maximum effectiveness of the continuity plan, DMR central office should work in conjunction with the regional offices to implement a comprehensive plan, periodically review the plan, when needed, modify the plan, and provide appropriate staff at regional offices, area offices, and facilities training in the plan's use.

We determined that physical security and environmental protection controls over on-site storage for critical and important computer-related media at the Hogan Regional Center and North Shore and Merrimack Valley area offices needed to be improved. We acknowledge that electronic backup by the central office would enable the Hogan and the area offices to reconstruct

client information. However, adequate on-site storage would enable DMR to restore processing in a much more timely manner.

AUDIT RESULTS

1. Business Continuity Planning

Our audit disclosed that although the DMR's Region III had performed certain preliminary steps regarding the development of a business continuity plan, Region III management, in conjunction with DMR's central office, needed to strengthen controls regarding business continuity planning. We found that DMR's "Internal Control Plan" required that "appropriate disaster recovery plans (be) in place for the Department's Electronic Data Processing (EDP) including off-site safeguarding of software and systems backup." However, the "Internal Control Plan" did not provide a cross-reference to a recovery and contingency plan that outlined detailed procedures to restore normal business functions to DMR offices in the event of long-term loss of automated systems. Further, we determined that physical security and environmental protection controls over on-site storage for critical and important computer-related media at the Hogan Regional Center and North Shore and Merrimack Valley area offices needed to be improved.

We determined that Region III had informally classified certain potential disaster scenarios related to the file servers and associated microcomputer systems installed at the Hogan facility and area offices and assessed their effects on the functioning of its computer operations. We found that management had informally designated certain applications, such as critical incident reports, individual service plans for DMR clients, and the client-related data warehouse processed on the DMR central office's file servers and the client registry system operating on the ITD mainframe critical systems related to client services. Further, Region III had developed informal procedures to process various transactions at alternate sites should automated systems at the Hogan facility or area offices or telecommunication links to the central office be unavailable for an extended period. For example, according to Region III management, they have used automated systems at area offices to process client or financial-related information when automated systems located at the Hogan facility or communication links to central office file servers were unavailable. Area offices have also used automated systems at Region III's offices to access applications on the central office's file servers. Further, Region III management has designated the State Police offices as an additional alternate site to access applications such as the client registry system or the Massachusetts Management Accounting and Reporting System (MMARS) operating on ITD's mainframe.

Our audit indicated, however, that a formal criticality assessment had not been performed nor control practices regarding alternate processing sites or user area plans documented. Further,

we determined that no documented procedures were in place, including instructions regarding the replacement of the file servers or microcomputer systems should the equipment be rendered inoperable and instructions for the staff to follow should the hardware fail to function.

Our audit indicated that on-site storage of computer-related media such as client funds, case notes, client information, and administrative correspondence at the Hogan facility and the North Shore and Merrimack Valley area offices needed to be improved. We found that at the Hogan facility backup media was stored in an open safe that was hot, lacked any environmental controls such as air-conditioning, and was cluttered with supplies and old microcomputers. Further, the safe was located in the MIS office that was open during normal business hours. We determined that at the North Shore area office backup media was kept in a desk drawer and at the Merrimack Valley area office backup media was placed on the office's file server. We found that the Merrimack Valley area office sends its backup media weekly to the Hogan facility. The North Shore area office did not use off-site storage for computer-related media.

We acknowledge that DMR's central office has implemented control practices regarding backup of computer-related media for regional and area offices that mitigate the potential loss of backup tapes stored at the Hogan facility or the area offices. All regional and area office file servers are backed up electronically on a daily basis. Further, according to DMR management, the Department recently began to send backup media weekly from the central office in Boston and regional offices to an off-site location. We found that the provisions for off-site storage of backup media were not consistently followed by the area offices reviewed. The loss of backup media at the Hogan facility and area offices could significantly hamper client services and the processing of administrative and financial transactions. Although the availability of backup is improved by daily electronic backup and weekly off-site storage, significant additional time would be required to reconstruct information from these sources compared to backup maintained in a secure on-site location.

A business continuity plan should document the DMR's recovery strategies with respect to various disaster scenarios. Without a comprehensive, formal, and tested recovery and contingency plan, including required user area plans, communication components, and ready availability of backup media, critical client services provided through Region III's administrative office, Hogan facility and the area offices could be significantly impeded.

The objective of business continuity planning is to help ensure the continuation of mission-critical functions should a disaster cause significant disruption to computer operations. Business continuity planning for information services is part of business continuity planning for the entire organization. Generally accepted practices and industry standards for computer operations support the need for each entity to have an ongoing, business continuity planning process that

assesses the relative criticality of information systems and develops appropriate contingency and recovery plans, if required. To that end, the entity should assess the extent to which it is dependent upon the continued availability of information systems for all required processing or operational needs and develop its recovery plans based on the critical aspects of its information systems.

The success of the business continuity planning process requires management commitment. Senior management and system users should be closely involved in business continuity planning to help ensure that there is a clear understanding of the entity's information system environment, that determinations of system criticality and the risks and exposures associated with the systems are correct, that appropriate data processing and user area plans are developed based on the relative criticality and importance of systems, and that adequate resources are available. Region III, in conjunction with the DMR central office, should perform a risk analysis of the systems and clearly understand the impact of lost or reduced processing capabilities. The risk analysis should identify the relevant threats that could damage the systems, the cost of recovering the systems, and the likelihood of the threat and frequency of occurrence.

Recommendation:

We recommend that Region III, in conjunction with the DMR central office, strengthen current procedures to ensure that the criticality of all automated systems and information technology is evaluated. Further, business continuity requirements should be assessed on an annual basis or upon major changes to user requirements or the automated systems.

We recommend that senior management and key users review currently defined recovery strategies to ensure that all mission-critical and important processing is addressed. We recommend that documented business continuity plans be tested to the extent necessary to provide reasonable assurance that recovery effects can be attained. Based on the results of a comprehensive criticality assessment, the DMR should complete the development of a written business continuity plan, including designated alternate processing sites and user area plans, for mission-critical and important functions.

The business continuity plan should document DMR’s recovery strategies with respect to various disaster scenarios. The recovery plan should contain all pertinent information needed to effectively and efficiently recover critical operations within the needed time frames. At a minimum, Region III should document user area plans for its administrative offices locate at the Hogan facility and area offices within the region to continue its operations should file servers or microcomputer systems be unavailable or telecommunication links to the central office be unavailable. We further recommend that the business continuity plan be tested, then periodically

reviewed and updated when needed to ensure that it is current, accurate, and complete. DMR staff should be trained in the execution of the plan under emergency conditions. The completed plan should be distributed to all appropriate staff members.

We recommend that procedures be implemented to ensure that criticality and associated risks and exposures of automated systems are evaluated annually or upon major changes to user requirements or the automated systems.

Regarding on-site storage at the Hogan facility and the two area offices reviewed, we recommend that DMR management make every effort to find a physically secure and environmentally protected on-site location for computer-related media. We recommend that DMR ensure that provisions for off-site storage of backup media be appropriately and consistently followed by area offices.

Auditee's Response:

> *Our Director of MIS, Karen Kelly, will consult with John Vasily, CIO at DMR Central Office, to determine the most efficient and effective manner in which to develop, a business continuity plan for the Region that will be in accord with central office plans and resources. Because some initiatives would require standard software utilization or programming, it would be impractical to implement these initiatives locally without discussion and review with Central Office MIS. In conjunction with Central Office, the Region will develop additional policies regarding password formation and use (there are existing policies regarding length of passwords and frequency of change) and for review of unauthorized attempts to access the network. When practices and policies are developed, it will be requested that they be included in the DMR internal control documentation. The resulting Business Continuity plan will document steps to be taken to respond to system demands and emergencies and will contain written, formal procedures that guard data integrity, and confidentiality. At a minimum, the business continuity plan will formalize and document contingency plans for the administrative offices located at the Regional Office and the Area Offices within the Region so that they may continue operations should file servers or microcomputer systems be unavailable or telecommunication links to the central office be unavailable.*

Auditor's Reply:

We are pleased that Region III management, in conjunction with DMR's central office, will develop a documented business continuity plan for administrative offices located at the regional office and area offices within the region. In addition, we agree with DMR's decision to develop additional policies and procedures regarding password formation and use and for monitoring of unauthorized attempts to access the network, and to include the documented controls in the internal control plan. We will review business continuity planning at our next scheduled audit.

Appendix
Summary of Internal Control Practices
Department of Mental Retardation
Region III
as of November 30, 2001

Page Ref	Control Area	Control Objective	Control Activities	Status of Control	Documented	Adequacy of Documentation
11	System Access Security	Provide reasonable assurance that only authorized users are granted system access to the automated systems	Passwords required to access automated systems, changes of passwords required at least every 60 days; formal rules for password formation and use; formal procedures for deactivation of logon IDs and passwords	In Effect	Yes	Adequate
11	Inventory Control over IT-related Resources	Provide reasonable assurance that property and equipment are properly safeguarded, accounted for in the inventory record, and reported on, when appropriate, to oversight department	Maintenance of an up-to-date inventory record; hardware tagged with state ID tags; annual physical inventory and reconciliation performed	In Effect	Yes	Adequate

Status of Control-Key:

In Effect = Control in place sufficient to meet control objective.

None = No internal control in place.
Insufficient = Partial control in place but inadequate to meet control objective.

Adequacy of Documentation-Key:
Adequate = Standard or guideline sufficient to describe, review, and follow significant controls.
Inadequate = Standard or guideline insufficient to describe, review, and follow significant controls.
N /A = Not Applicable

Appendix
Summary of Internal Control Practices
Department of Mental Retardation
Region III
as of November 30, 2001

Page Ref	Control Area	Control Objective	Control Activities	Status of Control	Documented	Adequacy of Documentation
11,12	Physical Security: o Hogan Regional Center, Administration Building o North Shore Area Office o Merrimack Valley Area Office	Provide reasonable assurance that only authorized staff can access business offices, computer rooms, microcomputer systems, and client records in hardcopy form so that, loss or damage is prevented	Control over access to offices, computer rooms, file servers, and microcomputer systems, designated facilities manager, intrusion devices, locked doors, foot patrols	In Effect, Key mgmt. procedures at Hogan need review	Yes	Inadequate
12	Environmental Protection: o Hogan Regional Center, Administration Building o North Shore Area Office o Merrimack Valley Area Office	Provide reasonable assurance that IT-related resources adequately protected form loss or damage	Proper ventilation, fire alarms, fire extinguishers, temperature controls, water sprinklers, posted emergency procedures	In Effect	Yes	Inadequate
13,15	Business Continuity Planning	Provide reasonable assurance that Region III can restore essential and mission-critical functions in a timely manner should file servers and microcomputer systems be rendered inoperable.	Current, formal, tested business continuity plan; periodic review and modification of plan; plan implemented, distributed, and staff trained in its use	Insufficient	No	N/A

Appendix
Summary of Internal Control Practices
Department of Mental Retardation
Region III
as of November 30, 2001

Page Ref	Control Area	Control Objective	Control Activities	Status of Control	Documented	Adequacy of Documentation
13,15	On-site storage	Provide reasonable assurance that computer related media is available should computer systems be rendered inoperable	Computer-related media backed up nightly; appropriate records maintained of backup; physical access security and environmental protection of storage are adequate; storage area is a separate on-site location	Insufficient	No	N/A
13,15	Off-site storage o Hogan Regional Center, Administration Building	Provide reasonable assurance that critical and important computer-related media are available should computer systems be rendered inoperable	Same as above. Storage area in a separate location	Off-site storage location not reviewed for Hogan	No	N/A
	o North Shore Area Office			None		
	o Merrimack Valley Area Office			Insufficient		

\